

Lab 3 - Port Security

Lab 3: Port security

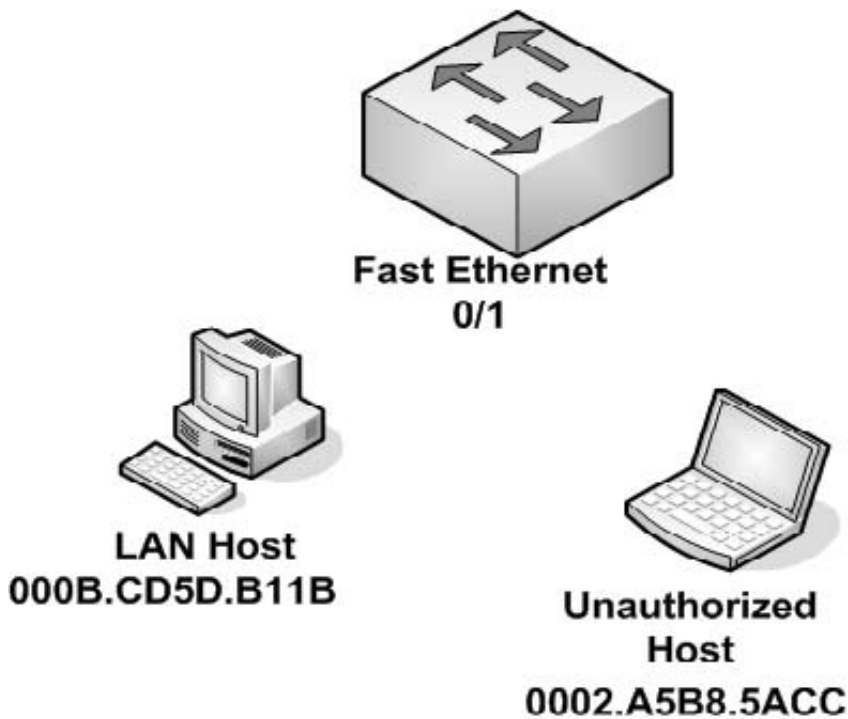


Figure 13-3: Port Security

Lab exercise

A PC is connected directly to the fast Ethernet 0/1 interface of your switch. You apply port security permitting only the LAN Host to connect through the port and a static MAC address. If a violation is detected, then the port should be shut down. You plug in the unauthorized host to check the configuration is working correctly.

Purpose

Security is very crucial for any network. Layer 2 security will ensure that no one can compromise the security from inside the network. You will be expected to know how to configure port security for the CCNA exam.

Lab objectives

1. Enable Port Security on fa0/1 on the switch.
2. Configure a static MAC address for port security on fa0/1.
3. Configure violation action on switchport.
4. Test the port by connecting a different device.

Lab walk-through

1. Enable Port Security on fa0/1 on the switch.

```
Switch#configure terminal
```

```
Switch(config)#interface fa0/1
```

```
Switch(config-if)#switchport port-security
```

(Note--the port you apply this command to must be an access and not trunk. If the interface is connected to another switch the switch may convert to trunk. The "show interfaces trunk" command will display your trunk interfaces:

```
Switch#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	desirable	802.1q	trunking	1

If you attempt to apply the command to a non-access port you will see the below output.

```
Switch(config-if)#switchport port-security
```

Command rejected: Not eligible for secure port.

To set an interface into access mode please apply the command:

```
Switch#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#int fast 0/1
```

```
Switch(config-if)#switchport mode access
```

2. Configure a static MAC address for port security on fa0/1. This will be the MAC address we want to permit to pass traffic through the switch port. You will need to alter the MAC address for your own.

```
Switch(config-if)#switchport port-security mac-address 000b.cd5d.b11b
```

(Note--you have several other options here. You can set the maximum number of mac addresses permitted through the switch port, hard set the mac address and the action upon violation of your settings (see step 3):

```
Switch(config-if)#switchport port-security ?
```

```
mac-address    Secure mac address
```

```
maximum        Max secure addrs
```

```
violation      Security Violation Mode
```

```
<cr>
```

3. Configure violation action on switchport. You may choose from restrict (inform the network admin

of the violation), shutdown or protect (only permit frames from the permitted devices.

Switch(config-if)#switchport port-security violation ?

protect Security violation protect mode

restrict Security violation restrict mode

shutdown Security violation shutdown mode

We are going to have the port shutdown when it detects a restriction.

Switch(config-if)#switchport port-security violation shutdown

4. Now plug the authorized host (LAN host) into your switchport fast ethernet 0/1. After about 30 seconds the switchport light will go from amber to green and show as up. You can then check the port security status with the "show port-security" command.

Switch#

00:40:32: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

00:40:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface

FastEthernet0/1, changed state to up

Switch#

Switch#show port-security int fast 0/1

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 1

Sticky MAC Addresses : 0

Last Source Address : 000b.cd5d.b11b

Security Violation Count : 0

5. Unplug the authorized host and plug in the unauthorized host. Once frames reach the switch port it will be closed down.

Switch#

00:40:32: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

00:40:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch#

00:41:04: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/ 1, putting Fa0/1 in err-disable state

00:41:04: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0002.a5b8.5acc on port FastEthernet0/ 1.

00:41:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

6. The interface has been shutdown. You can now check the port security status.

Switch#show port-security int fast 0/1

Port Security : Enabled

Port Status : Secure-shutdown

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 1

Sticky MAC Addresses : 0

Last Source Address : 0002.a5b8.5acc

Security Violation Count : 0

7. To re-enable the interface plug the authorized host back in and then “shut” and “no shut” the fast Ethernet interface.

One last point. Please take some time to use the other port security commands. You can for example, permit a maximum number of MAC addresses through the port or choose a specific range of allowed addresses.

Running configuration

Switch1#sh run

Building configuration...

--output truncated--

hostname Switch

!

```
interface FastEthernet0/1
```

```
switchport mode access
```

```
switchport port-security
```

```
switchport port-security violation shutdown
```

```
switchport port-security mac-address 000b.cd5d.b11b
```

!



© 2006-2011 HowtoNetwork.net All Rights Reserved. Reproduction without permission prohibited.